L’AIDE-MÉMOIRE DE LA CYBERHYGIÈNE POUR LA MAISON INTELLIGENTE

Nos maisons sont de plus en plus intelligentes. C’est génial! Mais ce qui est encore plus génial, c’est être aussi intelligent que sa maison intelligente.

La pire des catastrophes serait qu’un cybercriminel puisse déverrouiller nos serrures intelligentes ou pirater nos caméras intelligentes.

Voici donc notre aide-mémoire de la cyberhygiène pour la maison intelligente.

AVANT DE FAIRE QUOI QUE CE SOIT

Assurez-vous que vous devez effectivement vous connecter.
Le moyen le meilleur et le plus facile de vous protéger contre les dangers de l’ère numérique est de ne pas vous connecter si vous n’avez pas à le faire. Votre frigo doit-il vraiment pouvoir vous envoyer des messages textes? Votre grille-pain doit-il pouvoir prendre des autoportraits?

Faites une recherche avant d’acheter
La sécurité de votre maison intelligente commence par ce que vous achetez. C’est une bonne idée de vous en tenir, dans toute la mesure du possible, à des marques établies bien connues, dont le matériel a fait ses preuves. Recherchez des périphériques qui permettent de mettre facilement à jour les logiciels, de remplacer les mots de passe par défaut ou de désactiver les fonctions inutiles.

Faites installer vos périphériques par des professionnels.
Si le travail d'installation vous paraît trop compliqué, faites appel à des experts et confiez-leur le soin de s'assurer que vos périphériques intelligents sont installés en donnant la priorité à la sécurité.

PENDANT LE PARAMÉTRAGE

Inscrivez-vous auprès du fabricant.
Vous recevrez ainsi toutes les nouvelles mises à jour des logiciels. Aussi, assurez-vous de consulter les permissions qui ont été données pendant le paramétrage. Ne donnez pas accès à des périphériques auxquels il n'est pas nécessaire d'avoir accès.

Paramétrez un réseau pour les invités

Assurez-vous de donner à vos invités la possibilité de se connecter à un réseau distinct, qui n'est pas raccordé à vos périphériques de l'Internet de l'objet.

Protégez vos périphériques

Assurez-vous de remplacer votre nom d'utilisateur et votre mot de passe par défaut (ce qui est toujours une bonne idée). Aussi, désactivez les autres paramètres qui ne vous apportent aucun avantage, par exemple l'accès à distance, dont des cybercriminels pourraient se servir pour avoir accès à votre système.

L'authentification bifactorielle

Si vos applications de périphériques intelligents sont dotées de l'authentification bifactorielle, assurez-vous d'en profiter. Il s'agit pour vous d'un niveau supplémentaire d'authentification, en plus de votre

mot de passe. Il peut s'agir d'un code qui sera transmis à votre téléphone. L'authentification bifactorielle complique la vie des cybercriminels.

LES FACTEURS PERMANENTS DONT IL FAUT TENIR COMPTE

Les mises à jour!

Voici un conseil judicieux, quelle que soit la technologie : assurez-vous toujours que le logiciel de votre périphérique est à jour.

Vous devez connaître les périphériques que vous avez connectés. Le meilleur moyen d'avoir l'esprit tranquille avec des périphériques intelligents, c'est de connaître les périphériques que vous avez effectivement connectés à votre réseau domotique. Si vous ne les connaissez pas, fermez simplement votre Wi-Fi et prêtez attention aux périphériques qui cessent de fonctionner.

Pensez à une mise à niveau

Le moment est-il venu de mettre à niveau tout ce que vous avez déjà pour mieux sécuriser vos périphériques?

Attention aux pannes

Une panne de matériel peut nuire à la sécurité de vos périphériques. Assurez-vous de vérifier vos périphériques lorsque vous remarquez une panne.

Évitez les réseaux Wi-Fi publics

Les réseaux Wi-Fi publics sont super vulnérables aux attentats. Ne vous servez jamais de vos périphériques à partir d'une connexion avec un

réseau Wi-Fi public. Servez-vous de vos données ou d'un RPV sécurisé ou attendez de rentrer à la maison.

QUAND VOUS DÉMÉNAGEZ

Faites reparamétrer en usine vos périphériques avant de vous en défaire.

Quand vous décidez de jeter, de vendre vos périphériques intelligents ou de vous en défaire, assurez-vous de prendre les précautions nécessaires pour supprimer toutes les données qu'ils renferment. Ne permettez pas à leur prochain propriétaire de mettre la main sur ces données et ne leur donnez pas non plus la possibilité de communiquer avec d'autres périphériques de votre réseau.

Par Danny Pehar